



DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2021-0028]

Privacy Act of 1974: Implementation of Exemptions; U.S. Department of Homeland Security/ALL-046 Counterintelligence Program System of Records

AGENCY: U.S. Department of Homeland Security.

ACTION: Final rule.

SUMMARY: The U.S. Department of Homeland Security (DHS) is issuing a final rule to amend its regulations to exempt portions of a newly established system of records titled, “DHS/ALL-046 Counterintelligence Program System of Records” from certain provisions of the Privacy Act. Specifically, the Department exempts portions from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: This final rule is effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: For privacy questions please contact:

Lynn Parker Dupree, (202) 343-1756, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

The U.S. Department of Homeland Security (DHS) published a notice of proposed rulemaking in the Federal Register, 85 FR 80667 (December 14, 2020), proposing to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. In

concert with that rulemaking, DHS issued a new system of records notice, “DHS/ALL-046 Counterintelligence Program System of Records” in the Federal Register, 85 FR 80800 (December 14, 2020), outlining that DHS will collect and maintain records as part of the unified Counterintelligence Program across the Department.

DHS invited comments on both the Notice of Proposed Rulemaking (NPRM) and System of Records Notice (SORN).

II. Public Comments

DHS received no comments on the NPRM and comments from one organization on the SORN.

SORN

DHS received comments suggesting that (1) the scope of the proposed records system is broad and DHS components’ access to records covered by the Counterintelligence Program System of Records create the risk that components would use the records system in ways that exceed their stated missions; (2) the proposed routine use exemptions are not narrowly tailored to the defined purpose of the SORN for which the records are collected, would be used to disclose records to foreign and private entities that are not subject to the Privacy Act, and would create substantial risks for potential data breaches; (3) the Counterintelligence Program System of Records creates a substantial risk of data breach since the Federal Government has demonstrated it is incapable of handling and safeguarding sensitive information; and (4) the proposed exemptions are unnecessary and limit individuals’ ability to correct harmful errors, thwart DHS’s public notice obligations, and permit unlimited data collection, even if unnecessary and irrelevant. After full consideration of public comments, the Department will implement the rulemaking as proposed for the reasons described in the NPRM and as described here in the final rule.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS amends Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for part 5 continues to read as follows:

Authority: 6 U.S.C. sec. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. sec. 301. Subpart A also issued under 5 U.S.C. sec. 552. Subpart B also issued under 5 U.S.C. sec. 552a.

2. Amend Appendix C to Part 5 by adding paragraph 83 to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

83. The Department of Homeland Security (DHS)/ALL-046 Counterintelligence Program System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL-046 Counterintelligence Program System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities; and protection of the President of the U.S. or other individuals pursuant to Section 3056 and 3056A of Title 18. The system of records covers information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies.

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. secs. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8),

(e)(12); (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. secs. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

- (a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.
 - (b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities.
- Further, permitting amendment to counterintelligence records after an investigation has been completed would impose an unmanageable administrative burden. In addition, permitting access and amendment to such information could

disclose security-sensitive information that could be detrimental to homeland security.

- (c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.
- (d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.
- (e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.
- (f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

- (g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete.
- (h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.
- (i) From subsection (e)(12) (Matching Agreements) because requiring DHS to provide notice of a new or revised matching agreement with a non-Federal agency, if one existed, would impair DHS operations by indicating which data elements and information are valuable to DHS's analytical functions, thereby providing harmful disclosure of information to individuals who would seek to circumvent or interfere with DHS's missions.
- (j) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Lynn Parker Dupree,
Chief Privacy Officer,
U.S. Department of Homeland Security.